

An Observed-Data-Consistent Approach to the Assignment of Bit Values in a Quantum Random Number Generator

Pavel Lougovski* and Raphael Pooser

Quantum Information Science Group, Oak Ridge National Laboratory, Oak Ridge, TN 37831

The majority of Quantum Random Number Generators (QRNG) are designed as converters of a continuous quantum random variable into a discrete classical random bit value. For the resulting random bit sequence to be minimally biased, the conversion process demands an experimenter to fully characterize the underlying quantum system and implement parameter estimation routines. Here we show that conventional approaches to parameter estimation (such as e.g. *Maximum Likelihood Estimation*) used on a finite QRNG data sample without caution may introduce binning bias and lead to overestimation of the randomness of the QRNG output. To bypass these complications, we develop an alternative conversion approach based on the Bayesian statistical inference method. We illustrate our approach using experimental data from a time-of-arrival QRNG and numerically simulated data from a vacuum homodyning QRNG. Side-by-side comparison with the conventional conversion technique shows that our method provides an automatic on-line bias control and naturally bounds the best achievable QRNG bit rate for a given measurement record.

PACS numbers: 03.67.Hk, 03.67.Dd, 05.40.-a

I. INTRODUCTION

Random numbers are important for an array of applications from encryption and authentication systems [1], to Monte Carlo simulations for molecular dynamics, nuclear reactors, and others [2]. As a result, a variety of classical methods (computational pseudo-random number generators, sampling stochastic physical processes, etc.) to generate random number sequences have been developed. An attendant host of tests to certify that a given data sequence is “random” has been also been created [3–5]. While pseudo-random numbers are useful for many of these applications, including simulations and encryption with suitably high quality sources, their inherent determinism means that any encryption or authentication scheme is in principle breakable with sufficient computational power. This principle applies to any deterministic system, including processes described by classical physics.

On the other hand, the only nondeterministic physical theory with experimentally accessible applications is quantum mechanics [6]. The additional security provided by non determinism is a requirement for quantum key distribution, for instance, whose security proofs often rely on the concept of true, nondeterministic randomness in order to guarantee successful secret key sharing [7]. Thus, a wide array of so-called quantum random number generators (QRNG) have been developed. From radioactive decay [8] to quantum optical techniques [9, 10], a host of methods involving photon arrival time [11–14] and vacuum noise measurements [15, 16] have been demonstrated. Despite the prevalence of QRNGs and their acknowledged need, many implementations use extractors (such as hashes) to remove large amounts of bias compu-

tationally, exposing a potential weakness in their physical implementations. For instance, if an adversary is able to computationally reverse the extractor function that a given QRNG implements in order to achieve random number uniformity and the underlying (“physical”) distribution is strongly biased then he or she will have a best-guess strategy against the QRNG device. Therefore, one’s ability to detect and remove bias before applying an extractor function improves the QRNG’s security.

One of the major sources of bias in QRNGs, aside from environmental noise, is the lack of knowledge of precise values of the QRNG’s physical parameters. The best one may do is to estimate the parameters statistically. But because the estimates are statistical they are intrinsically noisy, and thus assigning a single value to a parameter can lead to errors and bias. Nevertheless, parameter estimator errors are usually ignored in QRNG design and simple point estimators are used. Here, we show that using point estimators may introduce possible binning bias. We argue that using a Bayesian statistical inference method removes this type of bias and propose a binning scheme that extracts the optimum number of bits possible for a given entropy from a given physical random number distribution. When used as a diagnostic for QRNGs in combination with maximum likelihood estimators (MLE), uniform distributions can be generated from sources of quantum randomness. Using Bayesian hypothesis updating techniques, our scheme allows for a test of the quantum model that produced a given set of numbers, potentially allowing for a fast, on-line quantum test of randomness. This technique has applications to high bit rate QRNGs which need testing and verification to ensure the device remains bias-free during use.

II. DIRECT BINNING FROM A CONTINUOUS DISTRIBUTION AND BIAS

Let X be a continuous random variable with probability density function (*pdf*) $f_X(x|\theta)$, where θ is a fixed-

*Electronic address: lougovskip@ornl.gov

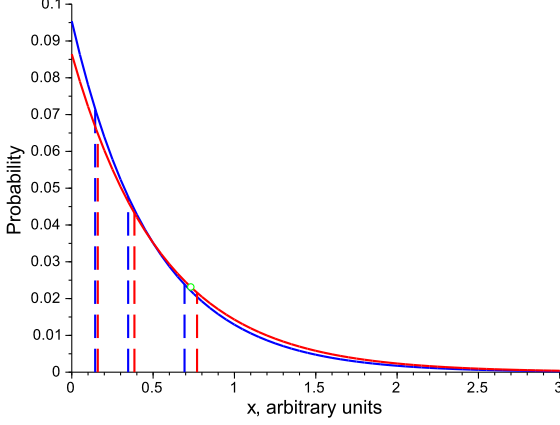


FIG. 1: Example of binning ambiguity for different values of distribution parameter.

(but unknown-) value parameter. The particular form and parametric dependence of $f_X(x|\theta)$ is determined by the experimental setup at hand. Our goal in this section is to introduce a typical problem of physical random number generation that can be formulated as follows: Provided M independent samples of X , $\{x_1, \dots, x_M\}$ are measured in an experiment, convert, if possible, each measurement outcome $x_i, i = 1, M$ into a discrete random variable $K = k_i$ with the probability mass function (pmf) $f_K(k)$ and corresponding domain $\mathcal{K} = \{1, \dots, N\}$. A uniform distribution $U(1, N)$ is often important in applications and here we will also concentrate on the case of $f_K(k) = U(1, N)$. Then the problem essentially reduces to constructing a surjection μ from the set $\mathcal{X} = \{x : f_X(x|\theta) > 0\}$ onto the set $\mathcal{K} = \{k : f_K(k) = 1/N, k = 1, \dots, N\}$.

Traditionally, the problem is solved by dividing the domain of $f_X(x|\theta)$, \mathcal{X} , into N mutually non-intersecting bins such that $\mathcal{X} = \{B_1 \cup \dots \cup B_N\}$ [18]. When bins are selected such that the probability of the random variable X to fall into the i -th bin B_i is

$$P(X \in B_i|\theta) = \int_{B_i} dx f_X(x|\theta) = \frac{1}{N}, \forall i, \quad (1)$$

then the surjection $\mu : \mathcal{X} \rightarrow \mathcal{K}$ can be constructed by following a simple rule: If a measurement result $X = x' \in B_i$ for some i then we assign $K = i$. Of course this mapping works only if the value of the model parameter θ is known. Since it is usually not the case in the majority of experimental situations, the first order of business is to find a good estimate of the value of θ . In many cases, the number of possible ways to construct an estimator that provides an unbiased estimate of θ is infinite [19]. Moreover, it is not always possible to find an estimator that has minimal uncertainty, and often one is forced to choose one from a set of almost optimal candidates. In

practice the maximum likelihood estimator (MLE) is a common choice.

Given a set d of independent samples of X , $d = \{x_1, \dots, x_M\}$, we can introduce the *likelihood* function,

$$L(\theta|d) = \prod_{k=1}^M f_X(x_k|\theta). \quad (2)$$

The likelihood $L(\theta|d)$ indicates which values of θ are more likely given measurement data d . We can also compute, at least numerically, the value of θ that maximizes $L(\theta|d)$, provided the likelihood function is convex. The resulting estimator is MLE, i.e. $\theta_{MLE} = \max_{\theta} L(\theta|d)$.

Using θ_{MLE} as the “true” parameter value for binning purposes in Eq.(1) might at first appear as a reasonable choice, and this approach is a mainstay in QRNG design. But what happens if instead of θ_{MLE} one uses some other estimate θ' that differs from θ_{MLE} only slightly in the value of the likelihood, i.e. $|L(\theta'|d) - L(\theta_{MLE}|d)| \ll 1, \theta' \neq \theta_{MLE}$? Choosing θ' over θ_{MLE} will have an effect on the size of bins B_i generated via Eq.(1). We illustrate this situation in Fig. 1, where the random variable X follows gamma distribution $\Gamma(1, \theta)$ (i.e. $f_X(x|\theta) = \theta e^{-\theta x}$) and we are interested in converting each measurement outcome $X = x_i$ into a uniformly distributed discrete random variable K that can take on values $\{0, 1, 2, 3\}$. We fit the same measurement data using two slightly different values of the parameter θ . The red solid line represents the fit with $\theta_1 = 1.8$ and the blue solid line has $\theta_2 = 2.0$. The vertical dashed blue (red) lines represent bins calculated using Eq.(9) with $N = 4$ and $\theta = \theta_2(\theta = \theta_1)$. The green circle is a particular measurement outcome x_i that we would like to assign a discrete value k to. According to our previous discussion, $k = 3$ and $k = 2$ if we use values θ_2 and θ_1 respectively.

Now imagine that θ_1 and θ_2 are such that the likelihood function does not provide a reliable differentiation between them, i.e. $L(\theta_1|d) \approx L(\theta_2|d)$. Which value of k , if any, should we then adopt? There are four possible options:

- Choose $\theta = \theta_1$ when θ_1 is the true estimate ($k = 2$).
- Choose $\theta = \theta_2$ when θ_2 is the true estimate ($k = 3$).
- Choose $\theta = \theta_1$ when θ_2 is the true estimate ($k = 2$).
- Choose $\theta = \theta_2$ when θ_1 is the true estimate ($k = 3$).

The first two choices are trivial since they obviously result in a uniform pmf $f_K(k) = \frac{1}{4} \forall k$. The last two choices, however, generate a bias that distorts the uniformity of $f_K(k)$. To see that we calculate the probability of X occupying the i -th bin provided that $\theta = \theta_1$ is chosen when θ_2 is the true estimate,

$$P(X \in B_i|\{\theta = \theta_1|\theta_2\}) = P(X \in B_i|\theta = \theta_1 \text{ when } \theta_2 \text{ is the true estimate}) = \int_{x_i}^{x_{i+1}} dx f_X(x|\theta_1) = \left[\frac{N-i}{N} \right]^{\frac{\theta_1}{\theta_2}} - \left[\frac{N-i-1}{N} \right]^{\frac{\theta_1}{\theta_2}}, \quad (3)$$

where $N = 4$, $x_i = -\frac{1}{\theta_2} \ln(\frac{N-i}{N})$, and $i = 0, 1, 2, 3$. We notice that, by definition, $f_K(k=i) = P(X \in B_i | \{\theta = \theta_1 | \theta_2\})$. Similarly, if we choose $\theta = \theta_2$ when θ_1 is the true estimate then the i -th bin probability $\tilde{f}_K(k=i)$ reads,

$$\begin{aligned} P(X \in B_i | \{\theta = \theta_2 | \theta_1\}) &= \tilde{f}_K(k=i) = \\ P(X \in B_i | \theta = \theta_2 \text{ when } \theta_1 \text{ is the true estimate}) &= \\ \int_{x_i}^{x_{i+1}} dx f_X(x | \theta_2) &= \left[\frac{N-i}{N} \right]^{\frac{\theta_2}{\theta_1}} - \left[\frac{N-i-1}{N} \right]^{\frac{\theta_2}{\theta_1}}, \quad (4) \end{aligned}$$

where $x_i = -\frac{1}{\theta_1} \ln(\frac{N-i}{N})$. Finally, the plot of pmfs $f_K(k)$ and $\tilde{f}_K(k)$ in Fig. 2, calculated using Eqs.(3) and (4) respectively for $N = 4$, illustrates the effect of parameter under(over)-estimation on the uniformity of the random numbers generated using the continuous distribution binning method. The horizontal axis represents the bin number k where a measurement outcome x_i is placed as the result of binning. The vertical axis is the probability for different values of k to occur. Ideally, if the value of θ was known exactly, the probability of $k = 0, 1, 2$, or 3 would be the same at $\frac{1}{4}$. This situation is represented by the solid blue line. When the value of θ is overestimated, $\tilde{f}_K(k)$ – the corresponding pmf in Eq.(4) – depicted by green crosses, exhibits a bias towards placing measurement outcomes into the first two bins. In a similar fashion, $f_K(k)$ in Eq.(3), represented by red circles, corresponds to the situation when the parameter θ is underestimated and demonstrates bias towards $k = 3$. To quantify the amount of introduced bias we compute values of Kullback-Leibler (KL) divergence $D_{KL}(\tilde{f}_K(k) || U(1, 4))$ and $D_{KL}(f_K(k) || U(1, 4))$ between the bin pmf $\tilde{f}_K(k)$ ($f_K(k)$) and the ideal uniform pmf $U(1, 4) = \frac{1}{4}$ respectively. By definition, KL divergence measures the information lost when the uniform pmf $U(1, 4)$ is used to approximate $\tilde{f}_K(k)$ or $f_K(k)$. We find that $D_{KL}(\tilde{f}_K(k) || U(1, 4)) = 0.006$ bits and $D_{KL}(f_K(k) || U(1, 4)) = 0.0059$ bits.

This example shows that discrete random number generation procedures relying on binning a continuous probability distribution with a parametric dependence potentially introduces bias. This happens because the point parameter estimation approach is prone to over(under)-estimating the true value of the parameter. Hence, the question arises: Is there a binning method that does not introduce bias? The short answer is yes, and such a method will be introduced in Section IV. In the next section, a slightly different approach to binning is shown in order to motivate the discussion.

III. UNIFORM RANDOM NUMBERS VIA INTEGRAL TRANSFORM

A measurement outcome $X = x_i$ does not depend on the value of the pdf parameter θ . However, the probability of the outcome does. As we have already seen, this means that the size of the bins also depends on θ , which

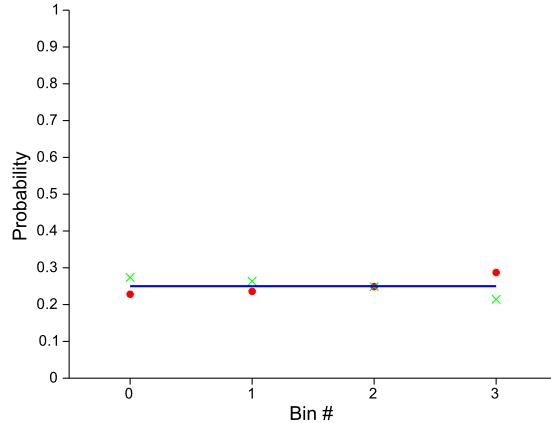


FIG. 2: Example of bias due to parameter estimation uncertainty.

makes binning procedure problematic. The reverse situation would be more practical, in which the bin size is fixed (independent of θ) but the measurement outcome depends on the pdf parameter. Of course, this does not remedy the problem of bias discussed earlier, but it will be useful in formulating a solution in the next section.

For a given fixed value θ , the probability $P(X \leq x | \theta)$ that the continuous random variable X is less than x reads,

$$P(X \leq x | \theta) = \int_{-\infty}^x dt f_X(t | \theta) \quad (5)$$

where we have assumed that $X \in (-\infty, +\infty)$. By definition $P(X \leq x | \theta) \in [0, 1]$ and $U = U(x) = P(X \leq x | \theta)$ can be interpreted as a uniform continuous random variable on the $[0, 1]$ interval provided $P(X \leq x | \theta)$ is a continuous function of x . The proof is straightforward and can be found elsewhere [19]. On the other hand, if the value of x is fixed, e.g. $x = x'$, and the value of θ is unknown then $U = P(X \leq x' | \theta) = U(\theta | x')$ is clearly a function of θ with the range $[0, 1]$.

If we divide the $[0, 1]$ interval into N uniform bins, each of the size $1/N$, then for every measurement outcome $X = x_i$ a discrete random number $K = k, k = \{1, \dots, N\}$ can be generated by finding k such that $(k-1)/N \leq U(\theta | x_i) < k/N$. This is exactly what we were looking for. By replacing the random variable X with U using the integral transform in Eq.(5) we switched from having bins that explicitly depended on the model parameter θ to having constant bin size. The parametric dependence is now shifted to the random variable that we bin, i.e. $U(\theta)$, and now we need to figure out a way to assign a value to $U(\theta)$ which does not create bias.

IV. BAYESIAN INFERENCE AND BINNING-BIAS-FREE RANDOM NUMBERS

We could try to fix the value of $U(\theta)$ by using an estimate of θ (e.g. MLE) as was done previously in Section II. However, this approach is inherently flawed because any finite data sample estimator – though it can be very close to the true parameter value – will over(under)-estimate the true parameter value. However, the concept of likelihood, or, more precisely, the concept of treating the distribution parameter θ as an unknown (but not random) variable given a set of measurements $d = \{x_1, \dots, x_M\}$ can be inverted using Bayesian inference to compute the probability $U(\theta)$ of occupying a given bin i .

Indeed, the Bayesian approach treats θ as a quantity whose variation is described by a probability distribution $\pi(\theta)$ usually referred to as the *prior*. The prior is a subjective distribution determined by experimenter's personal beliefs and knowledge about the system of interest prior to any observations on the system. Once $\pi(\theta)$ is formulated, an observation on the system is made. The prior is then updated with the result of the observation using Bayes rule and the next measurement is taken with the updated prior, often called *posterior*, as the new prior. If the sampling distribution, i.e. the distribution we draw measurement outcomes from, is $f_X(x|\theta)$ (the pdf to observe $X = x$ as a result of our measurement, given the parameter value θ) and the measurement result is $X = x$ then the posterior distribution is given by

$$\pi(\theta|x) = \frac{f_X(x|\theta)\pi(\theta)}{m(x)}, \quad (6)$$

where $m(x)$ is the marginal distribution of X :

$$m(x) = \int d\theta f_X(x|\theta)\pi(\theta). \quad (7)$$

The posterior distribution can be subjectively interpreted (since it does depend on the choice of the prior) as a conditional distribution (conditioned on the observed sample) for the parameter θ . On the other hand, we know that $U(\theta)$ is a function of θ given the measurement outcome $X = x$. Therefore, $U(\theta)$ can also be interpreted as a random variable on $[0, 1]$ with distribution function $g_U(u|x)$ that can be computed using $\pi(\theta|x)$,

$$g_U(u|x) = \pm \pi(U^{-1}(u)|x) \frac{dU^{-1}(u)}{du}, \quad (8)$$

where the plus (minus) sign is taken when $U(\theta)$ is an increasing (decreasing) function of θ , U is assumed to be continuous, and U^{-1} has a continuous first derivative. Now we are fully equipped to calculate the probability that a measurement outcome $X = x_i$ converts into an integer k ($k \in [1, N]$). It is equivalent to the probability that the random variable $U(\theta|x_i)$ falls into the interval

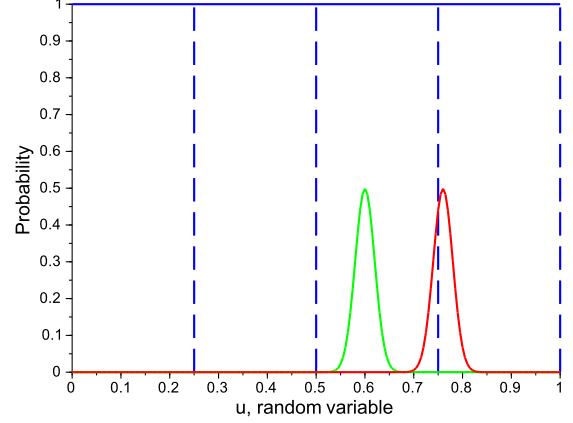


FIG. 3: Example of measurement acceptance/rejection based on $U(\theta)$ probability distribution.

$[(k-1)/N, k/N)$ given by,

$$\begin{aligned} P(x_i \rightarrow k) &= P\left(\frac{k-1}{N} \leq U(\theta|x_i) < \frac{k}{N}\right) = \\ &= \int_{\frac{k-1}{N}}^{\frac{k}{N}} g_U(u|x_i) du. \end{aligned} \quad (9)$$

This means that we now can assign a bin to a measurement outcome using a simple acceptance/rejection test: We accept x_i into the k -th bin if $P(x_i \rightarrow k) \geq P_a$ and reject x_i in the k -th bin otherwise. Here P_a is the user-defined acceptance probability. The binning bias can be completely eliminated by setting the value of P_a high ($P_a \geq 0.95$). This means that only the measurement outcomes that have more than 95% of their distribution function $g_U(u|x_i)$ localized within a certain bin will be accepted and converted into a discrete random number. All other measurements will be rejected. On the other hand, if P_a is set too low, say, $P_a < 0.5$ then less measurements will be rejected. However, this may lead to conflicting situations when a measurement outcome could be placed into two or more different bins which, in turn, may lead to binning bias.

Let us consider an example depicted in Figure 3 where two distribution functions $g_U(u|x_1)$ (red solid line) and $g_U(u|x_N)$ (green solid line) for two independent samples x_1 and x_N are plotted. We are interested in converting each measurement outcome x into an integer value $\{0, 1, 2, 3\}$. Using our acceptance/rejection test with $P_a = 0.95$ we conclude that x_N is an acceptable measurement that can be converted to $k = 2$. On contrary, x_1 will be rejected and no integer value will be assigned to it.

We finally summarize our approach to QRNG data processing as the following 5 step algorithm:

1. Run QRNG and collect M independent samples

$d = \{x_1, \dots, x_M\}$ from the distribution $f_X(x|\theta)$ defined by the QRNG.

2. Construct a prior $\pi(\theta)$ for all possible values of θ .
3. Update the prior M times using the Bayes rule Eq.(6). Compute the posterior $\pi(\theta|d)$.
4. For each measurement outcome x_i compute the correspondent distribution $g_U(u|x_i)$ using Eq.(8) and Eq.(5). Set the acceptance probability value P_a
5. Use the proposed acceptance/rejection test to convert the measured sequence d into integer values.

It is worth mentioning that alternatively, instead of waiting to collect a measurement record d , one could choose to update the prior on-line i.e. after each measurement. In this case it is likely that a few first measurement results will be discarded as we accumulate information about the QRNG device at hand. However, after enough information is received to narrow down the parameter distribution, it will be possible to convert upcoming measurements into random bit values.

V. EXAMPLES

To illustrate how our approach works in an experiment we consider two physical implementations of QRNGs. We first introduce mathematical models to describe the QRNGs of interest in the Section V A and then proceed with the analysis of the experimental data and numerical simulations results in Section V B.

A. Physical Models of QRNGs

1. Photon Time-of-Arrival QRNG

Let us first consider a QRNG based on measuring time-of-arrival statistics of a coherent light source. Our experimental setup consists of a tapered amplifier, emitting spontaneously and subsequently attenuated to a coherent state, that continuously illuminates the surface of a free-running single photon counting module with 80 ns dead time [20]. Using a gated FPGA essentially acting as a time to digital converter, we measure the time interval τ between two consecutive photodetection events. The time interval τ plays the role of a physical random variable X that we would like to convert into a discrete uniform random variable.

To determine statistical properties of τ , a quantum model of photodetection process is needed. For this purpose we introduce a positive-operator valued measure (POVM) $\{\hat{P}_0, \hat{P}_{click}\}$, where $\hat{P}_0 = |0\rangle\langle 0|$ is a projection operator that corresponds to “no-click” measurement of the detector and $\hat{P}_{click} = \sum_{k=1}^{\infty} |k\rangle\langle k|$ represents a “click” detection event. Note that $\hat{P}_{click} + \hat{P}_0 = \mathbb{1}$.

Then the detector click rate (i.e the click probability per unit time) reads,

$$\frac{dP_{click}}{dt} = \theta \text{Tr}[\rho_l \hat{P}_{click}], \quad (10)$$

here ρ_l is the density operator of the laser field and θ describes the overall detection efficiency. Therefore, the probability to get a click in a short time interval δt is $P_{click} = \theta \delta t \text{Tr}[\rho_l \hat{P}_{click}]$. On the other hand, the probability to detect no click in the same time interval is $P_0 = 1 - P_{click}$. Next consider the time interval τ between two consecutive detector clicks. We can model the absence of clicks during time τ by a sequence of N successful “no-click” measurements each of the duration $\delta t = \tau/N$. Hence, the probability to observe no clicks during time τ reads,

$$P_0(\tau) = \left(1 - \frac{\tau \tilde{\theta}}{N}\right)^N, \quad (11)$$

where we introduced $\tilde{\theta} = \theta \text{Tr}[\rho_l \hat{P}_{click}]$. In the limit of large N we obtain,

$$P_0(\tau) = \lim_{N \rightarrow \infty} \left(1 - \frac{\tau \tilde{\theta}}{N}\right)^N = e^{-\tilde{\theta}\tau}. \quad (12)$$

We now can compute the conditional probability to detect a click at $t = \tau$ given a click was detected at $t = 0$,

$$P(\tau|0) = \frac{P_{click}(t = \tau)P_0(\tau)P_{click}(t = 0)}{P_{click}(t = 0)} = \tilde{\theta} \delta t e^{-\tilde{\theta}\tau}. \quad (13)$$

Finally, the probability density $f(\tau|\tilde{\theta})$ for the random variable τ can be obtained by taking a derivative of $P(\tau|0)$,

$$f(\tau|\tilde{\theta}) = \frac{dP(\tau|0)}{d\tau} = \tilde{\theta} e^{-\tilde{\theta}\tau}. \quad (14)$$

Two main assumptions were made in the derivation of Eq.(14). First, the detection events are independent and identically distributed. This assumption is justifiable in case of moderate laser powers. Second, we have assumed noiseless detection. The later assumption is, unfortunately, not very realistic.

Avalanche photodiode detectors usually introduce two main sources of noise that affect the value of τ – afterpulsing and timing jitter. Afterpulsing is a false detection event in which electrons that were trapped by quenching in a previous detector gate are rereleased in subsequent detector gates, usually occurring after a true click due to a photon absorption event. The time interval τ_a between a true detection and an afterpulse event can be well characterized experimentally and the raw data can be filtered to remove the afterpulsing events by only accepting measurements with $\tau \geq \tau_a$. The filtering procedure effectively results in rescaling of the probability density in Eq.(14),

$$f(\tau|\tilde{\theta}) = \tilde{\theta} e^{-\tilde{\theta}(\tau - \tau_a)}, \quad (15)$$

where τ_a is a characteristic afterpulsing time.

The time jitter is a small error in the measurement of τ . The recorded time interval between two sequential clicks τ_r is a sum of two random variables $\tau_r = \tau + \tau_j$, where τ is the “true” time interval with pdf $f(\tau|\tilde{\theta})$ given in Eq.(15) and τ_j is a time jitter random $\mathcal{N}(0, \sigma_j^2)$ variable. One can show that the probability density for τ_r reads,

$$f(\tau_r|\sigma_j, \tilde{\theta}) = \tilde{\theta} e^{-\tilde{\theta}(\tau_r - \tau_a) + \frac{\sigma_j^2 \tilde{\theta}^2}{2}} \left[\text{erf}\left(\frac{\tau_r - \tau_a - \sigma_j^2 \tilde{\theta}}{\sqrt{2}\sigma_j}\right) - \text{erf}\left(\frac{\tilde{\theta}\sigma_j}{\sqrt{2}}\right) \right] \quad (16)$$

where erf denotes the error function. Notice that if the time jitter is small ($\sigma_j \rightarrow 0$), Eq.(16) coincides with Eq.(15). Since the observed time jitter is indeed small we will model the time-of-arrival QRNG using the probability density in Eq.(15) with one parameter $\tilde{\theta}$.

Let us also discuss how to implement the QRNG data processing algorithm described earlier for this model. The model pdf is given in Eq.(15). An obvious choice for the prior is a non-informative (uniform) prior $\pi(\tilde{\theta}) = \text{const}$ that assigns constant weight to all values of the parameter $\tilde{\theta}$. It turns out that in this case the posterior distribution $\pi(\tilde{\theta}|\tau_1, \dots, \tau_n)$ after n measurements can be calculated even analytically (instead of standard numerical updating) as,

$$\pi(\tilde{\theta}|\tau_1, \dots, \tau_n) = \Gamma(n+1, T) = \frac{\tilde{\theta}^n e^{-\tilde{\theta}T}}{T^{n+1}n!}, \quad (17)$$

where $T = \left(\sum_{k=1}^n \tau_k - n\tau_a \right)^{-1}$, and we assume that the characteristic afterpulsing time τ_a is known (not a parameter) and $\Gamma(n+1, T)$ denotes the gamma distribution function. Using Eq.(5) we introduce n random variables $u(\tilde{\theta}|\tau_1), \dots, u(\tilde{\theta}|\tau_n)$, where $u(\tilde{\theta}|\tau_i) = 1 - e^{-\tilde{\theta}(\tau_i - \tau_a)}$ and compute their probability distribution $g_i(u_i|\tau_i)$ using Eq.(8) and Eq.(17),

$$g_i(u_i|\tau_i) = \frac{[-\ln(1 - u_i)]^n (1 - u_i)^{\frac{1}{T(\tau_i - \tau_a)} - 1}}{n!(T(\tau_i - \tau_a))^{n+1}}. \quad (18)$$

And finally we calculate the probability $P(u_i \in j) = P(\frac{j-1}{N} \leq u_i \leq \frac{j}{N})$ that u_i falls into the j -th bin ($j \in [1, N]$)

$$P(u_i \in j) = \frac{1}{n!} \left[\gamma\left(n+1, -\frac{\ln(1 - j/N)}{T(\tau_i - \tau_a)}\right) - \gamma\left(n+1, -\frac{\ln(1 - (j-1)/N)}{T(\tau_i - \tau_a)}\right) \right], \quad (19)$$

where γ denotes the lower incomplete gamma function. Applying the acceptance/rejection test to $P(u_i \in j)$ for all pairs (i, j) will convert measurement outcomes τ_1, \dots, τ_n into a sequence of uniformly distributed integers on $[1, N]$.

2. Vacuum Quadrature Measurement QRNG

The second system that we consider here is a popular QRNG implementation based on vacuum quadrature measurement. Quantum vacuum fluctuations of the electromagnetic field are measured routinely at optical wavelengths using homodyne detection techniques [17]. A typical homodyne detector consists of a beam splitter with two input (I_1, I_2) and two output ports (O_1, O_2). Suppose that the input port I_1 carries a laser field described by a density operator ρ_L and the port I_2 carries the vacuum. By placing a photodetector in each of the output ports we measure the photon number difference operator \hat{N}_- between O_1 and O_2 ,

$$\hat{N}_- = [(\eta_1 t)^2 - (\eta_2 r)^2] a^\dagger a + [(\eta_1 r)^2 - (\eta_2 t)^2] b^\dagger b + rt(\eta_1^2 + \eta_2^2)[a^\dagger b + ab^\dagger], \quad (20)$$

where t (r) are the transmittance (reflectance) of the beam splitter, $\eta_{1,2}$ are detector 1,2 detection efficiencies and a^\dagger, a (b^\dagger, b) are creation/annihilation operators for the input port I_1 (I_2). Therefore, in a general experimental situation, \hat{N}_- will depend on three parameters r, η_1, η_2 (note that $t^2 = 1 - r^2$) and the laser field ρ_L . But since we only perform a numerical simulation of an experiment here and thus can “control” the parameters perfectly, we will assume that we have a 50/50 beam splitter ($t^2 = r^2 = 0.5$) and 100 percent efficient detectors ($\eta_1 = \eta_2 = 1$). We will also assume that the laser field is in a coherent state, i.e. $\rho_L = |\alpha\rangle\langle\alpha|$. Therefore, the expectation value of \hat{N}_- ,

$$\langle\hat{N}_-\rangle = |\alpha|\langle 0|be^{-i\phi_\alpha} + b^\dagger e^{i\phi_\alpha}|0\rangle = |\alpha|\langle 0|\hat{X}(\phi_\alpha)|0\rangle, \quad (21)$$

is proportional to the expectation value of the vacuum quadrature operator $\hat{X}(\phi_\alpha)$. Setting $|\alpha| = 1$ we conclude that by measuring the photon number difference in the output ports O_1 and O_2 we effectively measure the vacuum X quadrature, and hence, a particular measurement outcome in a normal random variable x_{vac} with pdf $\mathcal{N}(0, \sigma_{vac}^2)$.

In reality measurement results are always affected by electronic noise. The noise is usually model by a normal distribution $\mathcal{N}(0, \sigma_e^2)$ and thus the outcome of the quadrature measurement is a sum of the “true” quadrature random variable and the noise i.e. $x_r = x_{vac} + x_e$. Since x_{vac} and x_e are independent and normally distributed, their sum x_r is also a normally distributed random variable with pdf $\mathcal{N}(0, \sigma_{vac}^2 + \sigma_e^2)$. Therefore, we will model the output of vacuum quadrature measurement based QRNG as a continuous random variable x_r with the distribution function $f(x|\sigma)$,

$$f(x|\sigma) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{x^2}{2\sigma^2}}, \quad (22)$$

where $\sigma^2 = \sigma_{vac}^2 + \sigma_e^2$ is an unknown parameter.

With the QRNG model at hand we can now discuss how to apply the data processing algorithm developed

in Section IV to the vacuum quadrature measurement QRNG. Once again we start by choosing a prior. We propose to use a non-informative prior $\pi(\sigma) = \text{const}$ as in the previous example. The posterior distribution $\pi(\sigma|x_1, \dots, x_n)$ after n measurements can then be calculated analytically and reads,

$$\pi(\sigma|x_1, \dots, x_n) = \frac{X^{\frac{n-1}{2}} e^{-\frac{X}{2\sigma^2}}}{\sqrt{2^{n-3}} \Gamma(\frac{n-1}{2}) \sigma^n}, \quad (23)$$

where $X = \sum_{i=1}^n x_i^2$ and $\Gamma(\frac{n-1}{2})$ denotes the gamma function.

The next step in our procedure is to introduce n random variables $u(\sigma|x_1), \dots, u(\sigma|x_n)$ that later on will be binned. Unlike the previous example, where Eq.(5) was used for that purpose, we will rely on *Box-Muller* transform [19] here. Recall that U_1 and U_2 , two independent uniform(0,1) random variables, can be converted into two independent normal $\mathcal{N}(0, 1)$ random variable X and Y using the following transformation,

$$\begin{aligned} X &= R \cos \theta & R &= \sqrt{-2 \ln U_1} \\ Y &= R \sin \theta & \theta &= 2\pi U_2, \end{aligned} \quad (24)$$

On the other hand, a pair of measurement outcomes x_{i1}/σ and x_{i2}/σ can be converted into two random variables $u_1(\sigma|x_{i1}, x_{i2}) = \exp(-\frac{x_{i1}^2 + x_{i2}^2}{2\sigma^2})$ and $u_2(\sigma|x_{i1}, x_{i2}) = \arctan(x_{i2}/x_{i1})/2\pi \in [0, 1]$. Since $u_2(\sigma|x_{i1}, x_{i2})$ does not depend on the parameter σ (it is constant for a given pair x_{i1}, x_{i2}), it can be immediately placed into the j -th bin that satisfies $(j-1)/N \leq u_2 \leq j/N$. As to $u_1(\sigma|x_{i1}, x_{i2})$ which indeed is a function of σ , we can derive its probability distribution function $g(u_1|x_{i1}, x_{i2})$ using the posterior distribution in Eq.(23),

$$g(u_1|x_{i1}, x_{i2}) = \left(\frac{X}{x_{i1}^2 + x_{i2}^2} \right)^{\frac{n-1}{2}} \frac{(-\ln u_1)^{\frac{n-3}{2}} u_1^{\frac{X}{x_{i1}^2 + x_{i2}^2} - 1}}{\Gamma(\frac{n-1}{2})}. \quad (25)$$

Finally, the probability $P(u_1 \in j) = P(\frac{j-1}{N} \leq u_1 \leq \frac{j}{N})$ that u_1 falls into the j -th bin ($j \in [1, N]$)

$$\begin{aligned} P(u_1 \in j) &= \frac{1}{\Gamma(\frac{n-1}{2})} \left[\gamma\left(\frac{n-1}{2}, -\frac{X \ln(\frac{j-1}{N})}{x_{i1}^2 + x_{i2}^2}\right) - \right. \\ &\quad \left. - \gamma\left(\frac{n-1}{2}, -\frac{X \ln(\frac{j}{N})}{x_{i1}^2 + x_{i2}^2}\right) \right], \end{aligned} \quad (26)$$

where γ is the lower incomplete gamma function. Applying the acceptance/rejection test to $P(u_1 \in j)$ for all j will convert u_1 into a uniformly distributed integer on $[1, N]$. Therefore, a pair of normally distributed outputs of the vacuum homodyne measurement x_{i1} and x_{i2} converts into two uniformly distributed integer random numbers j_1 and j_2 .

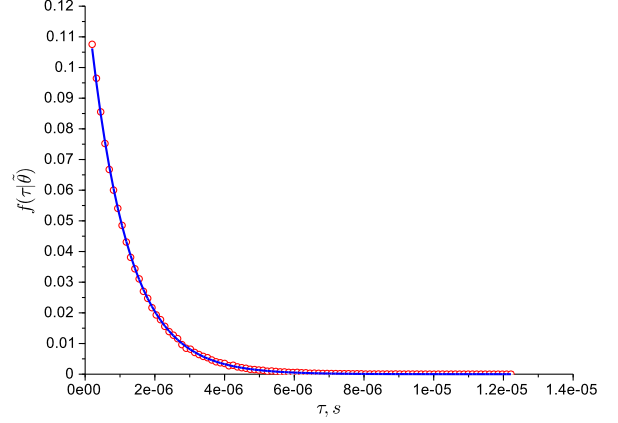


FIG. 4: Probability distribution of the time intervals between two successive detection events observed in the experiment.

B. Experimental Results and Simulations

1. Photon Time-of-Arrival QRNG

We collected a sample containing 256,000 measurements of the time interval between two consecutive detection events [20]. The raw data was filtered and all entries $\tau < \tau_a = 7.81 \times 10^{-8} s$ were removed from the sample to mitigate the effect of detector afterpulsing. The resulting filtered sample consisted of 221,890 measurements. We binned the filtered data into 100 bins of equal size $\Delta\tau = 1.225 \times 10^{-7} s$ and calculated the probability of each bin. The corresponding probability distribution is depicted in Fig. 4 with red circles. Based on the QRNG model discussed in Section V A 1 we calculated $\tilde{\theta}_{ML} = 9.16 \times 10^5 s^{-1}$, MLE for the parameter $\tilde{\theta}$. We used $\tilde{\theta}_{ML}$ in conjunction with the probability density function in Eq.(14) to fit the experimental data. The result is depicted on Fig. 4 with the solid blue line. Not surprisingly, given the number of measurements, the ML curve fits the data well.

Next we applied our data processing algorithm to the filtered data. We set the acceptance probability $P_a = 0.95$ and proceeded to convert the data into a set of 4-bit random numbers (i.e. measurement results are binned among $2^4 = 16$ bins). The number of measurements that passed acceptance/rejection criterion ($P \geq P_a$), and were assigned a bin value $(0, 1, \dots, 15)$, was 215,538 (out of 221,890). The resulting bin probability distribution is depicted in Fig. 5 using green triangles. The solid blue line corresponds to the ideal 4-bit uniform distribution and the red crosses represent a 4-bit probability distribution obtained from the same data set using the conventional fixed-parameter binning technique with $\tilde{\theta} = \tilde{\theta}_{ML}$. Both methods generate a visually uniform distribution. The uniformity is also confirmed by the values of Shan-

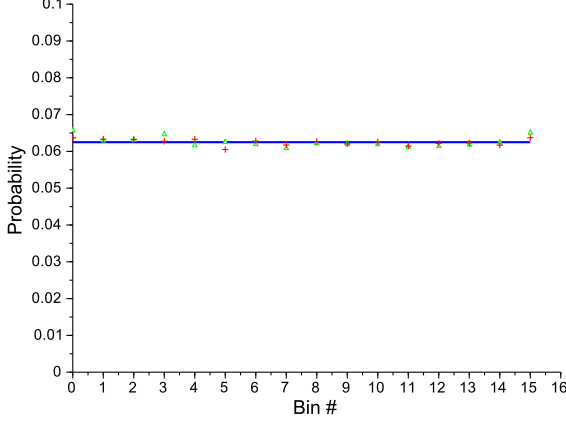


FIG. 5: Probability distribution of the 4-bit random numbers.

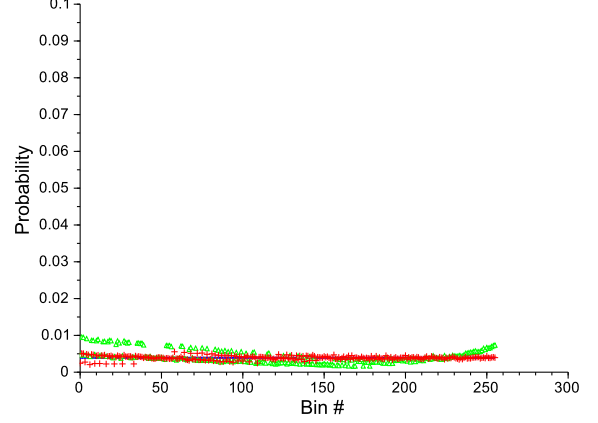


FIG. 7: Probability distribution of the 8-bit random numbers.

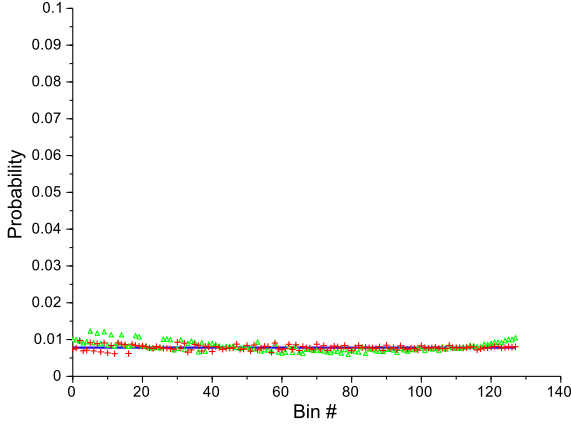


FIG. 6: Probability distribution of the 7-bit random numbers.

non entropy per bit – H – for each distribution. For the conventional binning $H = 0.999966$ bits and the entropy of the distribution generated by our binning method is $H = 0.999914$ bits.

In conventional bin assignment methods, once the distribution parameter value is estimated from a given set of measurements, the number of random bits that can be generated per single measurement is, in principle, only limited by the number of measurements [21]. This is because the mean error (standard deviation) of the parameter estimator is ignored in conventional binning. However, if the parameter estimation error is greater than the width of the bin where the measurement result is placed then such a bin assignment is erroneous and this measurement must be ignored and removed from the data. But this is exactly what our bin assignment method with the acceptance probability $P_a = 0.95$ does. It effectively

requires that the bin width should be greater than 4 standard deviations of the random variable u_i . If this requirement is not fulfilled the i -th measurement can not be assigned a bin reliably and the measurement is discarded. Hence, in contrast to the conventional binning our approach reduces the overall number of measurements. Therefore, for a given initial set of data, the number of random bits per measurement is naturally less in our method. In other words Bayesian updating provides a more conservative estimate of randomness of a QRNG when compared to ad-hoc binning. To illustrate this we generated 7- and 8-bit random number distributions from the same filtered data that we used for the 4-bit distribution above and the acceptance probability $P_a = 0.95$. The resulting distributions are depicted with green triangles on Fig. 6 and Fig. 7. As before the solid blue line corresponds to the ideal 7(8)-bit uniform distributions and the red crosses represent 7(8)-bit probability distribution obtained from the same size data sets using the conventional fixed-parameter binning technique with $\hat{\theta} = \hat{\theta}_{ML}$. The number of measurements that have passed acceptance/rejection criteria ($P \geq P_a$) is 172,736 (122,927) for the 7-(8)-bit distribution. We also calculated Shannon entropy for the conventional binning, $H_{7bit} = 7 \times 0.999314$ bits, and the entropy of our binning method is $H_{7bit} = 7 \times 0.997237$ bits. On the other hand the entropy in the 8-bit case for conventional binning is $H_{8bit} = 8 \times 0.998070$ bits and for the proposed binning method is $H_{8bit} = 8 \times 0.981067$ bits. As previously suspected, we observe a drop in the entropy of the 8-bit distribution generated using our technique. This implies that the collected data can reliably be converted into random bit sequences up to 7 bits long. Note that the conventional binning method does not provide us with such a conclusion.

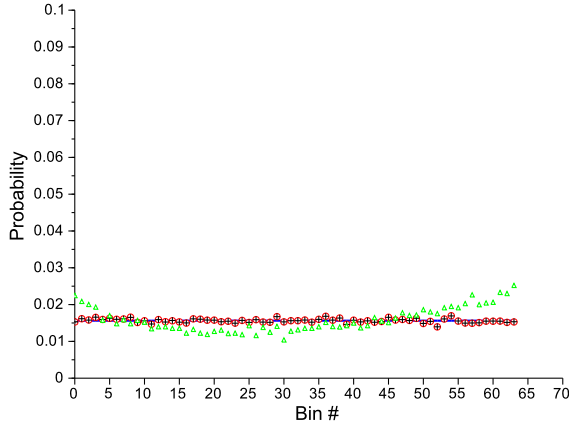


FIG. 8: Probability distribution of the 6-bit random numbers.

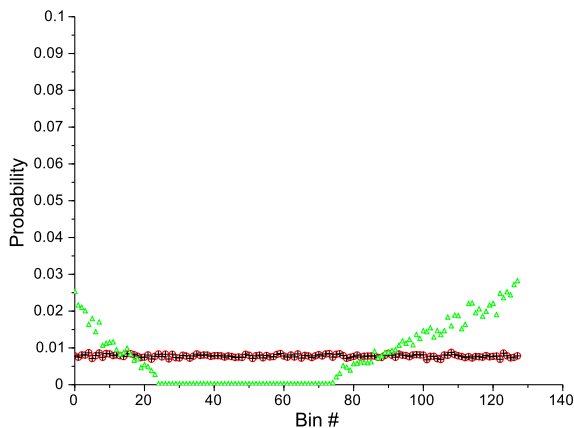


FIG. 9: Probability distribution of the 7-bit random numbers.

2. Vacuum Quadrature Measurement QRNG

We simulated vacuum homodyne measurements using a pseudo random number generator. Two independent sets of 50,000 random numbers were created by sampling the normal distributions $\mathcal{N}(0, \sigma_{vac})$ and $\mathcal{N}(0, \sigma_e)$ respectively. The first set with $\sigma_{vac} = 1$ represents noiseless vacuum quadrature measurement whereas the second set with $\sigma_e = 0.1\sigma_{vac}$ corresponds to the electronics noise.

Thus, the sum of the sets simulates the vacuum homodyning based QRNG that we previously modeled using Eq.(22).

We used the data to produce sets of 6- and 7-bit random numbers implementing both the conventional (MLE based) and proposed (Bayesian) binning methods. The resulting distributions are depicted in Fig. 8 and Fig. 9. The green triangles correspond to the probability distributions generated using our technique ($P_a = 0.95$), the red circles depict the results of the conventional MLE based binning and black crosses represent conventional binning with the “true” value of the parameter $\sigma^2 = 1.1$.

Examining Fig. 8 and Fig. 9 visually we observe that our method fails to produce a uniform 7-bit distribution indicating that the maximum number of random bits per measurement outcome cannot exceed 6 for the simulated data sample. This is also confirmed by the values of Shannon entropy $H_{6bit} = 6 \times 0.9945876$ versus $H_{7bit} = 7 \times 0.8668848$. Of course, generating a larger sample of measurements would allow a higher number of bits per measurement outcome as was the case in the previous Section. This illustrates the interplay between the number of measurement in a sample, acceptance probability, and the number of random bits that can be extracted from the sample.

VI. SUMMARY

In this manuscript we have demonstrated a new binning technique for QRNGs, as well as a formalized approach to characterize traditional binning methods. In particular, ad-hoc binning approaches are shown to result in possible bias when the model of the physical QRNG system is not taken into account. Using Bayesian hypothesis updating, a physical model can be used to quickly characterize experimental data. This has implications for new types of quantum statistical tests for randomness in a potentially more accessible manner than loop-hole-free Bell Inequality violation tests.

Acknowledgments

P. L. would like to thank Bing Qi, Ryan Bennink and Travis Humble for useful discussions. This work was performed at Oak Ridge National Laboratory, operated by UT-Battelle for the U.S. Department of energy under contract no. DE-AC05-00OR22725.

-
- [1] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, Handbook of Applied Cryptography, (CRC Press, London, 1997)
 - [2] J. H. Davenport, Papers from the international symposium on symbolic and algebraic computation Pages, ISSAC 123-129 (1992).

- [3] A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications,

NIST Special Publication 800-22.

- [4] see <http://www.stat.fsu.edu/pub/diehard/>
- [5] J. Walker, Ent tests, Fourmilab.ch. <http://www.fourmilab.ch/random/>
- [6] P. J. Bustard, D. Moffatt, R. Lausten, G. Wu, I. A. Walmsley, and B. J. Sussman, Opt. Exp. 19, 25173 (2011).
- [7] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. 74, 145 (2002).
- [8] H. Schmidt, Quantum mechanical random number generator, J. Appl. Phys. 41, 462468 (1970).
- [9] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, A fast and compact quantum random number generator, Rev. Sci. Instrum. 71, 16751680 (2000).
- [10] A. Stefanov, N. Gisin, L. Guinnard, and H. Zbinden, Optical quantum random number generator, J. Mod. Opt. 47, 595598 (2000).
- [11] M. Stipevia and B. Medved Rogina, Quantum random number generator based on photonic emission in semiconductors, Rev. Sci. Instrum. 78, 045104 (2007).
- [12] M. A. Wayne and P. G. Kwiat, Low-bias high-speed quantum random number generator via shaped optical pulses, Optics Express 18, 9351 (2010).
- [13] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. 93, 031109 (2008)
- [14] M. Wahl, M. Leifgen, M. Berlin, T. Rhlicke, H. -J. Rahn, and O. Benson, Appl. Phys. Lett., 98, 171105 (2011)
- [15] T. Symul, S. M. Assad, and P. K. Lam, Appl. Phys. Lett. 98, 231103 (2011)
- [16] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Maurer, U. L. Andersen, C. Marquardt, and G. Leuchs, Nat. Phot. 4, 711 (2010)
- [17] S. Pironio, A. Acn, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Nature 464, 1021-1024 (2010)
- [18] Feihu Xu, Bing Qi, Xiongfeng Ma, He Xu, Haoxuan Zheng, and Hoi-Kwong Lo, Opt. Exp. 20, 12366 (2012)
- [19] G. Casella and R. L. Berger, *Statistical inference* (Thomson Learning, 2002)
- [20] R. C. Pooser, P. G. Evans, T. S. Humble, IEEE Photonics Society Summer Topical Meeting Series, 147-148 (2013)
- [21] Increasing the number of bins N for a fixed number of measurements M also increases fluctuations in the probability of occurrence of a given bin, ultimately reducing the entropy of the distribution to zero.